基于不可信纠缠源的高斯调制连续变量量子密钥分发*

廖骎[1)] 柳海杰[1)] 王铮[1)] 朱凌瑾[2)†]

1) (湖南大学信息科学与工程学院, 长沙 410082)

2) (湖南省计量检测研究院, 长沙 410014)

(2022 年 9 月 30 日收到; 2022 年 11 月 21 日收到修改稿)

在实际的量子通信系统中, 连续变量量子密钥分发的信源安全可能会因为器件的缺陷或隐藏的攻击而受到威胁. 针对这个问题, 本文提出了基于不可信纠缠源的高斯调制连续变量量子密钥分发方案, 通过将高斯纠缠源置于不可信的量子信道来模拟纠缠源被攻击者所控制的场景, 从而验证实际复杂环境下高斯调制连续变量量子密钥分发的安全性. 本文详细分析不可信纠缠源对系统安全性的影响并引入了两种光学放大器来辅助提升所提方案的实际性能. 仿真实验结果表明, 本文所提方案即使在高斯纠缠源不可信的情况下仍然能够产生安全的量子密钥, 同时, 光学放大器也能够有效提升接收端探测器的量子效率. 该工作旨在推动高斯调制连续变量量子密钥分发系统的实用化进程, 为高斯调制连续变量量子密钥分发系统的实际部署和应用提供理论指导.

关键词: 连续变量量子密钥分发, 不可信纠缠源, 光学放大器, 量子通信

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.72.20221902

1 引 言

量子通信具有由量子力学原理保证的理论无条件安全性, 是量子信息领域的研究方向之一. 其中, 基于连续变量的量子通信技术凭借量子态易于制备、系统部署成本较低、兼容现代通信系统、信道容量高等优势成为研究的热点前沿[1]. 连续变量量子通信包括连续变量量子密钥分发协议[2,3]、连续变量量子会话协议[1,4]、连续变量量子密钥共享协议[5,6]、连续变量量子确定性密钥分发协议[7,8]等, 其中发展较快的是连续变量量子密钥分发协议. 量子密钥分发 (quantum key distribution, QKD) 允许两个合法的通信双方在不安全的量子信道上进行点对点的保密通信. 根据物理学中本征态具有的连续谱和离散谱两种不同的特征, QKD 主要可以分为离散变量 (discrete-variable, DV) QKD 和连续变量 (continuous-variable, CV) QKD 两大类. 在 CVQKD 中, 发送方 (Alice) 通常在光场的正则分量上采用高斯调制编码密钥信息; 接收方 (Bob) 则采用相干探测技术来恢复密钥[9]. CVQKD 继承了连续变量技术的优势, 使其得到了领域内研究者的广泛关注[10].

目前, 高斯调制 (Gaussian-modulated, GM) CVQKD[11–13] 协议具有比较完备的安全性分析方法且其理论无条件安全性已经得到了充分证明[14,15]. 然而, 由于实际器件的不完美性, 攻击者可以利用这些不完美器件发起针对于 GMCVQKD 实际系

* 国家自然科学基金项目 (批准号: 62101180)、湖南省自然科学基金项目 (批准号: 2022JJ30163) 和国防科技大学高性能计算国家重点实验室 (批准号: 202101-25) 资助的课题.

† 通信作者. E-mail: zhulingjin1020@foxmail.com

统的各种攻击, 严重阻碍了 GMCVQKD 的部署和应用进程. 已提出的针对于系统实际安全性发起的攻击主要有: 校准攻击[16]、本振光抖动攻击[17]、饱和攻击[18]、波长攻击[19,20]以及致盲攻击[21]等等. 对于这些攻击手段, 目前的防御策略主要是采取主动监控或增加光学器件来过滤攻击. 除此之外, 许多研究者通过将机器学习理论和技术引入 GMCVQKD 系统达到实时检测和防御实际攻击的目的[22,23]. 这些方法的确为 GMCVQKD 系统的实际安全性提供了有力保障. 然而, 在防范系统漏洞的同时, 一个重要的实际安全问题往往被忽略, 那就是信号源的安全性. 众所周知, GMCVQKD 的理论安全性证明的基本假设之一就是信号源必须完全可信, 即信号源无法被攻击. 但是, 在实际的网络环境中, 这个假设是不现实的, 就算信号源被掌握在可信的发送方手中, 也可能因为工作人员被策反等原因造成信号源被窃听者所控制. 为了解决这个问题, Weedbrook[24]证明了纠缠源置于不可信量子信道中间这一特殊情形下 CVQKD 的理论渐近安全性. Liao 等[23,25]在上述理论安全性证明的基础上, 提出了基于不可信纠缠源的离散调制的连续变量量子密钥分发方案并验证了大气信道下不可信纠缠源的连续变量量子密钥分发方案的可行性. 相比之下, 目前对 GMCVQKD 的信源安全性的研究尚不充分, 但是, 验证量子保密通信系统中高斯调制的纠缠源有可能被攻击的实际安全问题具有非常重要的意义, 有助于推进 GMCVQKD 系统的实际部署和应用. 另外, 在 CVQKD 系统中, 接收方 (Bob) 的探测器不可避免地存在一些固有缺陷, 无法达到理想的探测效率[26–28], 导致 CVQKD 系统实际性能的下降. 因此, 如何补偿由探测器缺陷造成的性能损耗, 也是提高 CVQKD 系统的实际性能重要方法.

基于以上分析, 本文提出基于不可信纠缠源的 GMCVQKD 方案, 并在此基础上, 通过部署光学放大器来补偿相干探测器的不完美缺陷, 提升系统的性能. 具体地, 通过将高斯纠缠源移出发送端并置于不可信的量子信道上来分析其安全性, 并在接收端的入口处部署相位敏感放大器 (phase-sensitive amplifier, PSA) 对零差探测器进行补偿和相位不敏感放大器 (phase-insensitive amplifier, PIA) 对外差探测器的进行补偿. 仿真结果表明: 在适当的距离下, 即使信源置于不安全的信道中, 通信双方仍然能产生安全密钥; 并且, 在部署两种放大器后, 接收端探测器的量子效率有了大幅的提升. 本文提出的方案为在实际环境中部署 GMCVQKD 的提供了理论指导, 有助于推动 GMCVQKD 系统的实用化进程.

本文首先详述了提出的基于不可信纠缠源的 GMCVQKD 方案和安全性分析, 并对方案的性能进行了详细分析, 最后介绍了使用放大器对探测器的补偿效果.

2 基于不可信纠缠源的 GMCVQKD

2.1 方案描述

图 1 展示了基于不可信纠缠源的 GMCVQKD 的方案图. 与图 2 的纠缠源可信的 GMCVQKD 方案[26]相比, 本文的方案通过将纠缠源移出发送端 Alice 的安全范围并将其置于不可信的量子信道来验证 GMCVQKD 系统的实际安全性. 在此基础上, 攻击者 Eve 可以制备或控制纠缠源并发动攻击. 因此, Eve 可以将 Alice 和 Bob 的量子信道替换成自己的量子信道并进行窃听[25]. 为了模拟信道损耗, Eve 使用了两个透射率分别为 T_1 和 T_2 的分束器, 如图 1 所示. 显然, 当 $T_1=1$ 时, 方案等价于纠缠源可信的 GMCVQKD方案, 而当 $T_1=T_2$ 时, 表示纠缠源位于信道正中间, 此时 Eve 针对通信双方的攻击是对称的, 因此, 信道的总透射率表示为 $T=T_1T_2$. 具体的方案步骤如下:

1) 首先假设纠缠源是高斯的, 并将纠缠源移出 Alice 端, 移至不可信的量子信道中.

2) 不可信信道内的纠缠源生成 EPR 对, 分别具有 A 和 B_0 两个模式, 将其分别发送给 Alice 和 Bob.

3) 假设 Eve 对信道两端的通信双方 Alice 和 Bob 发起纠缠克隆攻击[29], 该攻击在正向协商和反向协商下的最强攻击能力已经被证明[30–31].

4) Eve 制备方差为 $W_i(i=1,2)$ 的辅助态 $|E_i\rangle$ 并准备透射率为 $T_i(i=1,2)$ 的分束器, 将信道替换成自己的攻击信道. 其中攻击信道的透射率为 T_i, 过噪声与输入 ε 有关.

5) Eve 将其辅助态的其中一个模式 $|E_{i1}\rangle$ 保存在量子存储器中, 辅助态的另一个模式 $|E_{i2}\rangle$ 被注入各自分束器中未使用的端口, 并各自与发送给 Alice 和 Bob 的模式在分束器中进行光学混合. 随后 Eve 将其中一个端口的 A_1 模式和 B_1 模式分别发送给 Alice 和 Bob. Eve 得到输出模式 $|E_{i3}\rangle$ 后将其保存到量子存储器中[24,25].

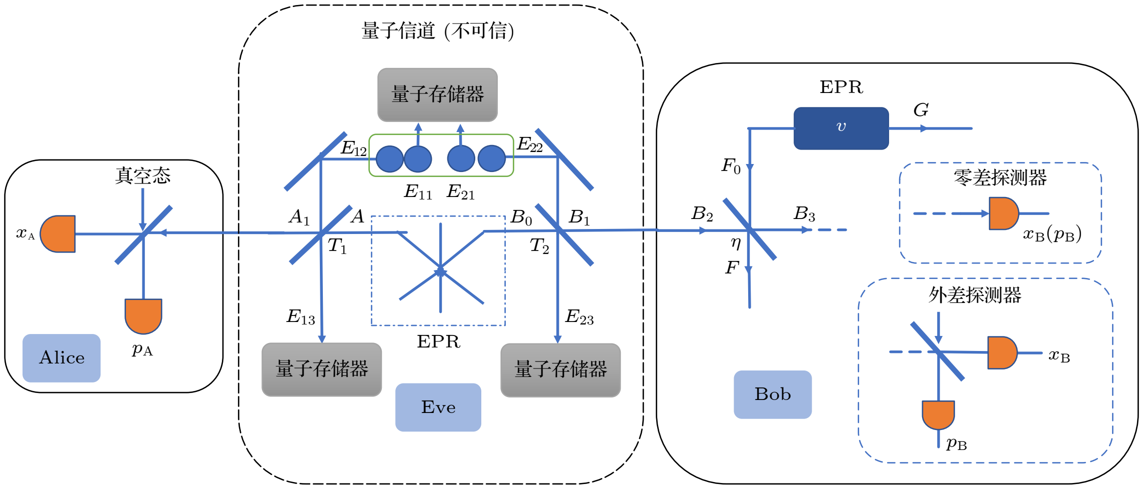

图 1 基于不可信纠缠源的 GMCVQKD 的方案图

Fig. 1. Scheme diagram of the GMCVQKD based on untrusted entanglement source.

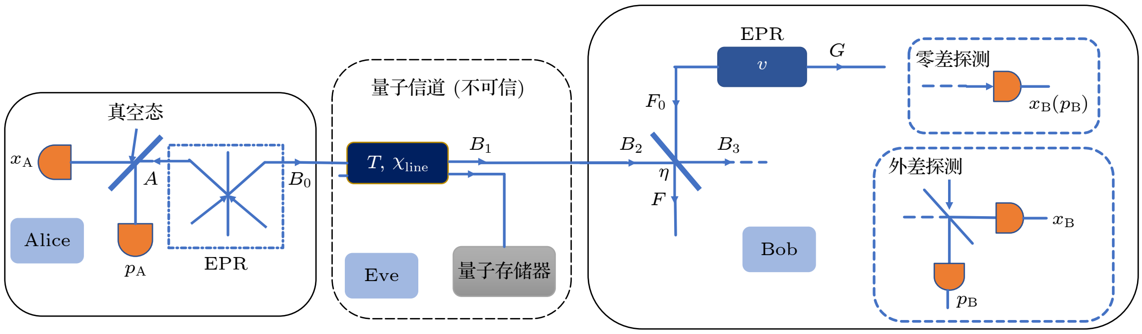

图 2 纠缠源可信的 GMCVQKD 的方案图

Fig. 2. Scheme diagram of the GMCVQKD with trusted entanglement source.

6) 最后, 当 Alice 和 Bob 通过经典的通信信道公布相关信息后, Eve 可以进行准确的测量从而得到有效的信息.

2.2 安全性分析

基于不可信纠缠源的 GMCVQKD 方案的渐近安全密钥率取决于通信双方 Alice 和 Bob 的协方差矩阵 $\gamma_{A_1B_1}$, 可表示为[26]

$$\gamma_{A_1B_1}=\begin{bmatrix} aI_2 & c\sigma_z \\ c\sigma_z & bI_2 \end{bmatrix}, \tag{1}$$

其中, $I_2=\text{diag}(1,1)$为二维单位矩阵, $a=T_1V+(1-T_1)W_1$, $b=T_2V+(1-T_2)W_2$, $c=[T_1T_2(V^2-1)]^{1/2}$, $\sigma_z=\text{diag}(1,-1)$, $W_i=T_i\chi_i/(1-T_i)$是关于输入$\chi_i=(1-T_i)/T_i+\varepsilon$的加性噪声, V表示 EPR 纠缠态的方差. 基于上述协方差矩阵, 本文所提方案在集体攻击下的渐近安全密钥率为[26]

$$R=\beta I_{A_1B_3}-\chi_{\text{BE}}, \tag{2}$$

其中β表示反向协商效率, $I_{A_1B_3}$表示通信双方 Alice 和 Bob 之间的香农互信息量, χ_{BE}表示 Bob 和 Eve 之间的互信息的 Holevo 界.

在方案采用零差检测的情况下, Alice 和 Bob 之间的互信息量为[26]

$$I_{A_1B_3}^{\text{hom}}=\frac{1}{2}\log_2\frac{V+\chi_{\text{tot}}}{1+\chi_{\text{tot}}}, \tag{3}$$

其中$\chi_{\text{tot}}=\chi_{\text{line}}+\chi_{\text{h}}$表示信道输入端的总噪声, $\chi_{\text{line}}=1/T+\varepsilon-1$表示信道输入端的加性噪声, $\chi_{\text{hom}}=[(1-\eta)+v_{\text{el}}]/\eta$表示零差探测器的噪声, 其中$\eta$和$v_{\text{el}}$分别表示 Bob 端探测器的量子效率和电噪声.

χ_{BE}界定了 Eve 能够从 Bob 端获取的最大信息量, 表示为[26]

$$\begin{aligned}\chi_{\text{BE}}&=S(\rho_{A_1B_1})-S(\rho_{A_1\text{FG}}^{m_B})\\&=\sum_{i=1}^{2}G\left(\frac{\lambda_i-1}{2}\right)-\sum_{i=3}^{5}G\left(\frac{\lambda_i-1}{2}\right),\end{aligned} \tag{4}$$

其中, $G(x)=(x+1)\log_2(x+1)-x\log_2 x$,

$$\lambda_{1,2} = \sqrt{\frac{1}{2}(\varDelta \pm \sqrt{\varDelta^2 - 4C})}, \tag{5}$$

$$\varDelta = a^2 + b^2 - 2c^2, \tag{6}$$

$$C = (ab - c^2)^2, \tag{7}$$

$$\lambda_{3,4} = \sqrt{\frac{1}{2}(O_{\text{hom}} \pm \sqrt{O_{\text{hom}}^2 - 4D_{\text{hom}}})}, \tag{8}$$

$$O_{\text{hom}} = \frac{\varDelta\chi_{\text{hom}} + V\sqrt{C} + T(V + \chi_{\text{line}})}{T(V + \chi_{\text{tot}})}, \tag{9}$$

$$D_{\text{hom}} = \sqrt{C}\frac{V + \sqrt{C}\chi_{\text{hom}}}{T(V + \chi_{\text{tot}})}. \tag{10}$$

当方案采用外差检测时, Alice 和 Bob 之间的互信息量表示为[26]

$$I_{A_1B_3}^{\text{het}} = \log_2\frac{V + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}}. \tag{11}$$

Bob 和 Eve 之间互信息的 Holevo 界 χ_{BE}与 (4) 式相同, 其特征值$\lambda_{1,2}$也与 (5) 式相同, 而特征值$\lambda_{3,4}$表示为[26]

$$\lambda_{3,4} = \sqrt{\frac{1}{2}(O_{\text{het}} \pm \sqrt{(O_{\text{het}}^2 - 4D_{\text{het}}})}, \tag{12}$$

$$O_{\text{het}} = \frac{1}{(T(V + \chi_{\text{tot}}))^2}\Big[\varDelta\chi_{\text{het}}^2 + C + 1 + 2\chi_{\text{het}}\Big(V\sqrt{C} + T(V + \chi_{\text{line}})\Big) + 2T(V^2 - 1)\Big], \tag{13}$$

$$D_{\text{het}} = \left(\frac{V + \sqrt{C}\chi_{\text{het}}}{T(V + \chi_{\text{tot}})}\right)^2, \tag{14}$$

其中外差探测器的噪声表示为$\chi_{\text{het}} = [1 + (1 - \eta) + 2\upsilon_{\text{el}}]/\eta$. 最后一个特征值$\lambda_5$在外差和零差探测的情况下均为 1.

2.3 性能分析

本节讨论了基于不可信纠缠源的 GMCVQKD 方案在渐近安全下的性能. 根据实际的实验环境, 仿真实验中的全局参数设定如下: EPR 纠缠态的方差为$V = 4$, 信道透射率$T = 10^{-\alpha L/10}$, 其中光纤衰减系数$\alpha = 0.2$ dB/km, L表示信道的长度, 探测器的量子效率和电子噪声分别为$\eta = 0.5$和$\upsilon_{\text{el}} = 0.01$, 协商效率$\beta = 0.97$, 系统的过噪声$\varepsilon = 0.01$[32–34].

图 3 对原始的 GMCVQKD 方案和纠缠源不可信的 GMCVQKD 方案在安全密钥率、互信息量和 Holevo 界 3 个方面进行性能的比较, 其中L_{Alice}=0 km 表示原始的 GMCVQKD 方案的仿真结果, $L_{\text{Alice}} =$ 0.01 km 和$L_{\text{Alice}} \to$ 0.01km 表示基于纠缠源不可信的 GMCVQKD 方案的仿真结果 (其中$L_{\text{Alice}} =$ 0.01 km 指纠缠源移出 Alice 端 10 m, 而$L_{\text{Alice}} \to$ 0.01km 表示纠缠源非常趋近于 Alice 端, 本文取值为 1 m). 从图 3(a) 可以看出, GMCVQKD方案在纠缠源不可信的情况下仍然能得到安全密钥率. 但是, 相较于原始的 GMCVQKD 方案, 方案的性能有明显地下降. 特别是, 一旦将纠缠源移出 Alice 的保护范围 (即使非常接近 Alice 方), 协议的最大传输距离就会降至 150 km 以下. 为探究造成这一现象的主要原因, 图 3(b) 比较了两种方案的互信息量, 发现两者的互信息量基本一致. 由 (1) 式可知, 造成最大传输距离下降的主要因素是 Bob 与 Eve 的 Holevo 界. 为此, 图 3(c) 展示了原始的 GMCVQKD 方案和纠缠源不可信的 GMCVQKD方案的 Holevo 界. 从图 3(c) 可观察到, 与原始的 GMCVQKD 方案相比, 不可信纠缠源的 GMCVQKD 方案的 Holevo 界有明显地增长, 这表明不可信的纠缠源增强了 Eve 集体攻击的能力. 因此, 一旦纠缠源移出 Alice 的合法范围, 方案的性能就急剧下降. 除此之外, 从图 3(c) 还可以看出, 纠缠源越接近 Alice 端, Holevo 界越高. 为了进一步探究纠缠源的距离对所提方案的安全密钥率的影响, 图 4 绘制了纠缠源置于不同位置的安全密钥率. 与原方案相比, 性能差距虽然明显, 但是随着纠缠源与 Alice 端距离 (L_{Alice}) 的增大, 所提方案的最大传输距离也逐渐增大. 特别地, 在图 4(a) 中可以看出所提方案的最大传输距离超过了 150 km. 这是因为 Holevo 界随着距离L_{Alice}的上升在逐渐减小, 甚至逐渐接近原始方案的 Holevo 界, 如图 4(b) 所示. 此外, 在不可信纠缠源的 GMCVQKD 中, W_i对系统的性能影响较大, Eve 可以根据实际的信道噪声χ_i对其进行调制和匹配并通过仔细控制过噪声的值, 使其在可容忍的门限值内, 从而隐藏自己的攻击. 因此, 探究W_i对系统性能的影响非常重要, 而W_i值的关键因素是过噪声ε. 为此, 图 5 仿真了零差探测下所提方案在不同ε下的安全密钥率. 从图 5 可以观察到, 过噪声越小, 方案的安全传输距离越大, 随着过噪声的增大, 方案的安全距离也逐渐减小, 尤其是当ε为 0.02 时, 方案的传输距离直接下降到 100 km 以下. 上述仿真的实验结果均是在零差探测下得到

的, 除此之外, 图 6 还给出了采用外差探测时不可信纠缠源的 GMCVQKD 的性能. 从图 6 可以看出, 当系统采用外差探测时, 不可信纠缠源的方案和原始方案的安全传输距离差距较大, 同时, 虽然该方案也能产生正向的安全密钥率, 但相较于采用零差探测的情况, 方案的最大传输距离有明显地下降. 例如, 当 $L_{\rm Alice}$ 等于 0.05 km 时, 采用零差探测的方案的最大传输距离超过 150 km, 而采用外差探测的方案的最大传输距离降至 150 km. 为了解释这一现象, 图 6(b) 给出了采用外差探测时不同 $L_{\rm Alice}$ 的 Holevo 界. 与零差探测类似, 外差检测的 Holevo 界也随着 $L_{\rm Alice}$ 的上升而减少, 并且逐渐与原始方案的 Holevo 界接近. 此外, 相较于零差探测, 外差探测的 Holevo 界有着非常明显的增加. 造成这一现象的原因可能是由于外差探测的噪声比零差探测的大, 而这部分噪声通常被视为攻击者 Eve 截获信息的一部分, 从而导致 Holevo 界的增加.

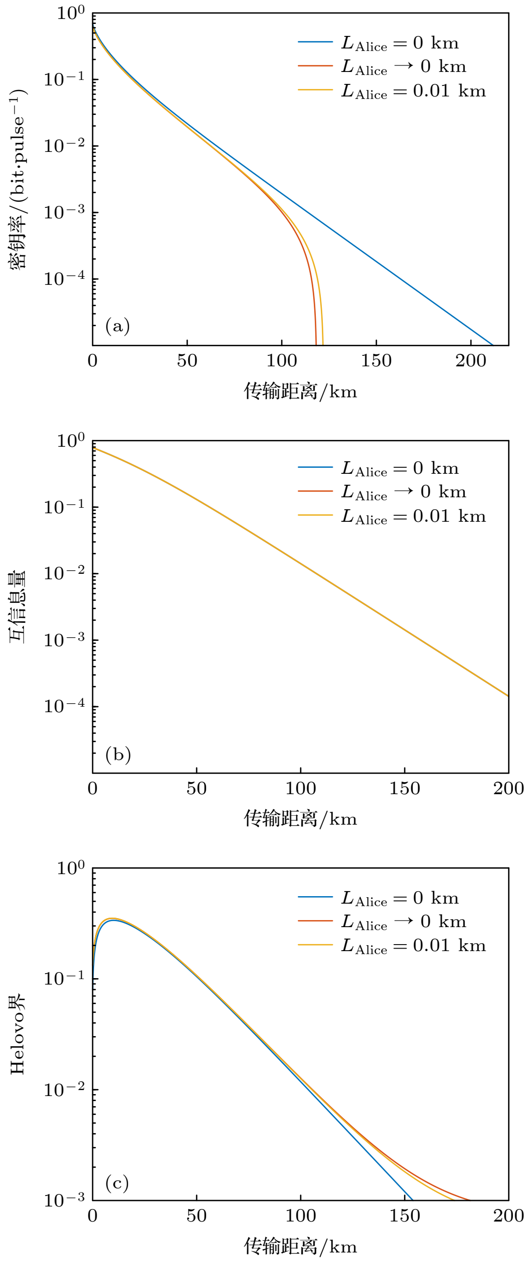

图 3 零差探测下不可信纠缠源的 GMCVQKD 方案的与原始 GMCVQKD 方案的性能对比 (a) 两种方案的安全密钥率与传输距离的关系; (b) 两种方案的互信量与传输距离的关系; (c) 两种方案的 Holevo 界与传输距离的关系

Fig. 3. The performance comparison between the GMCVQKD scheme with an untrusted entanglement source and the original GMCVQKD scheme under homodyne detection: (a) The relationship between the security key rate and transmission distance of the two schemes; (b) the relationship between mutual information and transmission distance of the two schemes; (c) the relationship between Holevo bound and transmission distance of two schemes.

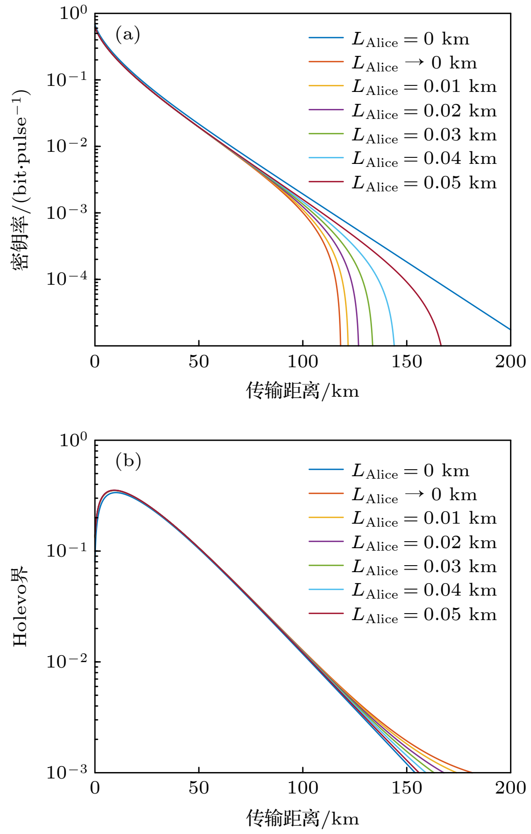

图 4 零差探测下基于不可信纠缠源的 GMCVQKD 方案在不同纠缠源距离下的性能 (a) 所提方案的安全密钥率与传输距离的关系; (b) 所提方案的 Holevo 界与传输距离的关系

Fig. 4. Performance of the GMCVQKD scheme based on an untrusted entanglement source with homodyne detection at different entanglement source distances: (a) Relationship between the security key rate of the proposed scheme and the transmission distance; (b) relationship between the Holevo bound of the proposed scheme and the transmission distance.

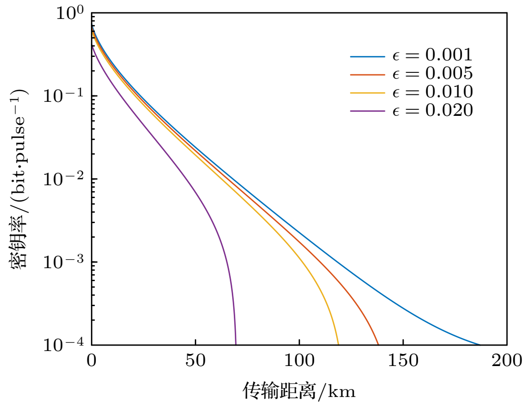

图 5 零差探测下基于不可信纠缠源的 GMCVQKD 方案在不同过噪声下的性能

Fig. 5. The performance of the GMCVQKD scheme based on an untrusted entanglement source under different excess noise.

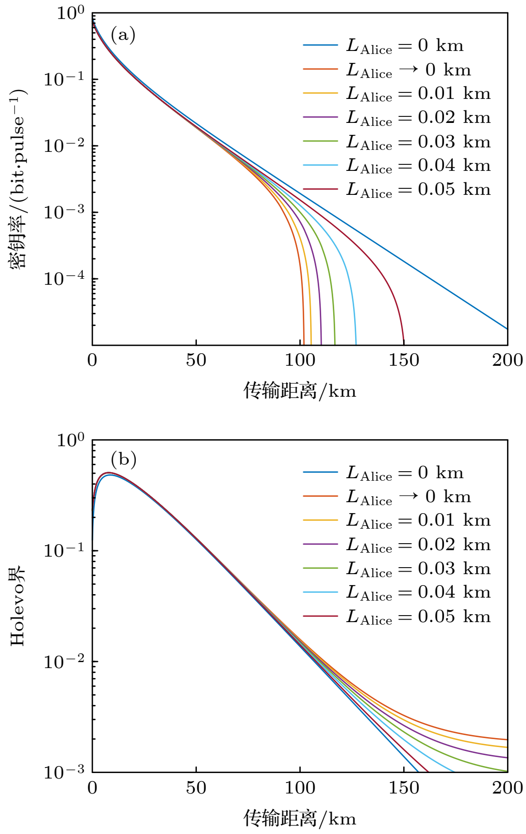

图 6 外差探测下基于不可信纠缠源的 GMCVQKD 方案在不同纠缠源距离下的性能 (a) 所提方案的安全密钥率与传输距离的关系; (b) 所提方案的 Holevo 界与传输距离的关系

Fig. 6. Performance of the GMCVQKD scheme based on an untrusted entanglement source with heterodyne detection at different entanglement source distances: (a) Relationship between the security key rate of the proposed scheme and the transmission distance; (b) relationship between the Holevo bound of the proposed scheme and the transmission distance.

3 光学放大器的补偿效应

光学放大器在量子密钥分发中的应用已经得到了广泛的研究[35–39], 本节针对基于不可信纠缠源的 GMCVQKD 系统中探测器存在的固有缺陷, 将 PSA 和 PIA 两个放大器应用于实际系统中以探究两种放大器对不理想探测器的补偿效应. 本节主要针对 PSA 与零差探测器以及 PIA 和外差探测器这两种组合配置进行分析. 其他两种组合配置在本节中暂不作讨论.

3.1 PSA 与零差探测组合后的性能分析

PSA 是一种简并光参量放大器, 其在理想情况下可以对选定的正交分量进行无噪声的放大[26]. 其放大过程描述为: $x_{\rm s} \to \sqrt{g}x_{\rm s}, p_{\rm s} \to p_{\rm s}/\sqrt{g}$, 其中, $g \geqslant 1$表示放大的增益系数, $x_{\rm s}$ 和 $p_{\rm s}$ 表示信号的两个正则分量, 其模型如图 7 所示. 下面针对 PSA 与零差探测器的组合配置进行性能分析.

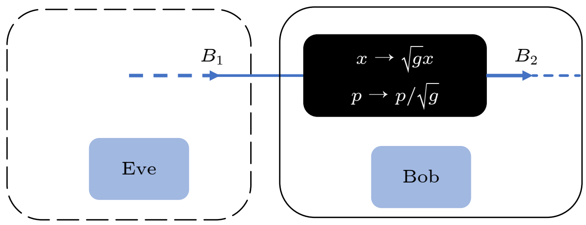

图 7 PSA 的模型

Fig. 7. Model of PSA.

如前所述, Eve 获得 Bob 的密钥信息量由 (4) 式推导得出, 然而 (4) 式的前半部分并不依赖于 Bob 端的设备, 因此, 最后的结果取决于 (4) 式的第 2 部分. 根据文献 [26], 当 Bob 使用 PSA 来补偿零差探测器时, 其特征值 $\lambda_{3,4}$ 的表达式与 (9) 式和 (10) 式一致, 唯一的改变是探测器的加性噪声. 因此, 添加 PSA 放大器后, $\chi_{\rm hom}$ 修改为[26]

$$\chi_{\rm hom}^{\rm PSA} = \frac{(1-\eta)+v_{\rm el}}{g\eta}. \tag{15}$$

根据 (15) 式, 图 8 给出了 PSA 和零差探测器组合下, 不可信纠缠源的 GMCVQKD 方案的安全密钥率的仿真结果. 图中由蓝色线代表没有放大器作用的情况, 紫色线表示系统具有理想的探测器的情况, 其他线则描述了插入 PSA 后安全密钥率在不同的放大增益系数 g (分别取 3, 20)[26] 下的仿真结果. 仿真结果表明, 当 PSA 的增益系数越大, 补偿

的效应就越明显, 特别地, 当增益系数为 20时, 其安全密钥率甚至可以与理想的零差探测器相媲美. 此外, 图 (8) 的插图中还展示了当增益系数 g=1 时 (即不添加 PSA 放大器), 其传输距离与添加 PSA 放大器后的差距, 特别地, 两者的安全传输距离差超过了 5 km. 因此, 可以表明, PSA 能够补偿零差探测器的内在缺陷, 同时, 在增益系数足够大的情况下, 一个理想的 PSA 甚至可以完全地补偿放大器的内在缺陷. 从系统的角度来说, PSA 和零差探测的组合可以视为一个理想的探测装置.

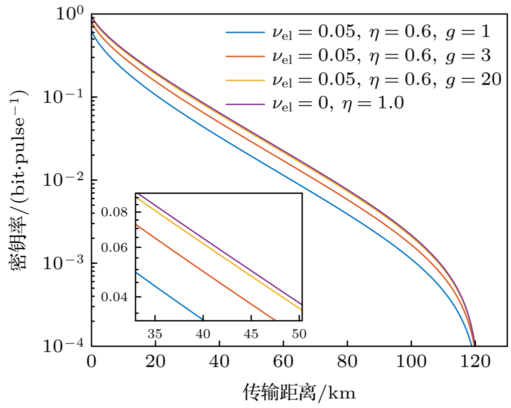

图 8 零差探测与 PSA 组合后的安全密钥率

Fig. 8. Security key rate for the combination of homodyne detection and PSA.

3.2 PIA 与外差探测组合后的性能分析

PIA 是非简并光参量放大器, 它可以对选定的正交分量进行同倍数放大[26]. 其放大过程描述为 $x_{\rm s}\rightarrow\sqrt{g}x_{\rm s}+\sqrt{g-1}x_{\rm I}$, $p_{\rm s}\rightarrow\sqrt{g}p_{\rm s}-\sqrt{g-1}p_{\rm I}$; $x_{\rm I}\rightarrow\sqrt{g}x_{\rm I}+\sqrt{g-1}x_{\rm s}$, $p_{\rm I}\rightarrow\sqrt{g}p_{\rm I}-\sqrt{g-1}p_{\rm s}$. 其中 S 和 I 分别表示信号模式和空闲模式, 其中空闲模式在理想状态下为一个真空态而在实际情况下是一个方差为 $V_{\rm I}$ 的态, 其模型如图 9 所示. 需要说明的是, PIA 模型是由增益因子为 g 的无噪放大器和一个方差为 N 的 EPR 态组成. 其内部噪声是通过将一半的 EPR 态注入放大器的第 2 个入口来模拟. 下面从安全密钥率的角度讨论 PIA 与外差探测器组合后系统的性能.

外差探测与 PIA 组合的性能分析和零差探测与 PSA 的组合类似, 只需考虑 (4) 式的后半部分. 不过, 两者的不同之处在于, 对外差探测与 PIA 进行性能分析时, 要额外考虑到 PIA 的加性噪声. 正如图 9 所示, (4) 式的计算中还需要包括模式 I 和 J. 因此, (4) 式重写为[26]

$$\begin{aligned}\chi_{\rm BE}=&S(\rho_{A_1B_1})-S(\rho_{A_1{\rm IJFG}}^{x_B;p_B})\\=&\sum_{i=1}^{2}G\left(\frac{\lambda_i-1}{2}\right)-\sum_{i=3}^{7}G\left(\frac{\lambda_i-1}{2}\right).\end{aligned}\tag{16}$$

其中, 特征值 $\lambda_{3,4}$ 的表达式与 (13) 式和 (14) 式的一致, 且 $\lambda_{5,6,7}=1$. 同样地, 外差探测器的加性噪声也发生了变化, 在 Bob 添加 PIA 放大器后, $\chi_{\rm het}$ 重写为[26]

$$\chi_{\rm het}^{\rm PIA}=\frac{1+(1+\eta)+2\upsilon_{\rm el}+N(g-1)\eta}{g\eta}.\tag{17}$$

根据 (17) 式, 图 10 仿真了在 PIA 和外差探测器组合下, 基于不可信纠缠源的 GMCVQKD 方案的安全密钥率的仿真结果. 图中深蓝色线代表不使用放大器的情况, 由浅蓝色线代表不使用放大器, 且探测器没有内部缺陷的情况, 其他线表示插入 PIA 后安全密钥率在不同的放大增益系数 g(分别取 3, 20)[26] 和放大器噪声 N (分别取 1, 1.5)[26] 下的结果. 从图 10 可以看出, 当 PIA 的增益逐渐增大, 由外差探测器内部缺陷带来的性能下降问题也逐渐得到了补偿, 当增益系数 g 取 20 时, 其性能甚至可以逼近理想探测器的情况. 此外, 插图显式地展示了不添加 PIA 放大器与插入 PIA 放大器的性

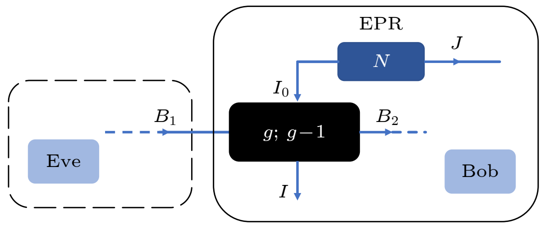

图 9 PIA 的模型

Fig. 9. Model of PIA.

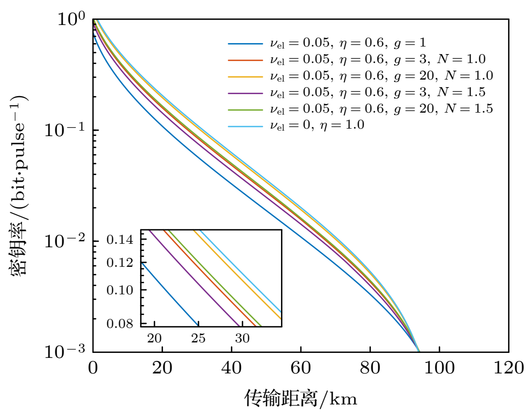

图 10 外差探测与 PIA 组合后的安全密钥率

Fig. 10. Security key rate for the combination of heterodyne detection and PIA.

能差距, 数据表明两者的安全距离差超过了 5 km. 另外, 在图 10 还可以观察到放大器的噪声 N 对系统的密钥率也有很大的影响, N 值越小, 密钥率越高. 从某种意义上来说, PIA 与外差探测器的组合也可以视为一个理想的探测设备.

4 结 论

本文提出了一个基于不可信纠缠源的 GMCVQKD 方案, 相比于传统方案, 本文提出的方案不再需要光源可信的假设条件, 而是通过将纠缠源移置不可信的量子信道并进行安全性分析, 验证了当发送端不可信或被 Eve 控制时 GMCVQKD 协议的安全性. 实验结果表明, 即使纠缠源置于不可信的量子信道中, 本文方案依然能够安全地分发密钥, 从而消除了 CVQKD 理论安全性分析中信号源必须可信的假设条件. 因此, 本文为 GMCVQKD 系统在实际复杂环境下的部署提供了理论依据, 具有更强的实用性, 有助于推动 GMCVQKD 的实用化发展. 此外, 针对检测器件的不完美缺陷, 本文分别通过部署 PSA 和 PIA 对相干探测器进行了补偿, 提升了基于不可信纠缠源的 GMCVQKD 系统的性能.

参考文献

[1] Zhou N R, Li J F, Yu Z B, Gong L H, Farouk A 2016 *Quantum Inf. Process* **16** 4

[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N, Peev M 2009 *Rev. Mod. Phys.* **81** 1301

[3] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[4] Gong L H, Li J F, Zhou N R 2018 *Laser Phys. Lett.* **15** 105204

[5] Liao Q, Liu H J, Zhu L J, Guo Y 2021 *Phys. Rev. A* **103** 032410

[6] Liao Q, Liu H J, Gong Y P, Wang Z, Peng Q Q, Guo Y 2022 *Opt. Express* **30** 3876

[7] Song H C, Gong L H, Zhou N R 2012 *Acta Phys. Sin.* **61** 154206 (in Chinese) [宋汉冲, 龚黎华, 周南润 2012 物理学报 **61** 154206]

[8] Zhou N R, Wang L J, Ding J, Gong L H, Zuo X W 2010 *Int. J. Theor. Phys.* **49** 2035

[9] Guo Y, Liao Q, Wang Y J, Huang D, Huang P, Zeng G H 2017 *Phys. Rev. A* **95** 032304

[10] Zhong H, Ye W, Wu X D, Guo Y 2021 *Acta Phys. Sin.* **70** 020301 (in Chinese) [钟海, 叶炜, 吴晓东, 郭迎 2021 物理学报 **70** 020301]

[11] Lance A M, Symul T, Sharma V, Weedbrook C, Ralph T C, Lam P K 2005 *Phys. Rev. Lett.* **95** 180503

[12] Ma X C, Sun S H, Jiang M S, Gui M, Liang L M 2014 *Phys. Rev. A* **89** 042335

[13] Grosshans F, Grangier P 2002 *Phys. Rev. Lett.* **88** 057902

[14] Leverrier A 2015 *Phys. Rev. Lett.* **114** 070501

[15] Leverrier A, Grosshans F, Grangier P 2010 *Phys. Rev. A* **81** 062343

[16] Jouguet P, Kunz-Jacques S, Diamanti E 2013 *Phys. Rev. A* **87** 062313

[17] Ma X C, Sun S H, Jiang M S, Liang L M 2013 *Phys. Rev. A* **88** 022339

[18] Qin H, Kumar R, Alléaume R 2016 *Phys. Rev. A* **94** 012325

[19] Huang J Z, Weedbrook C, Yin Z Q, Wang S, Li H W, Chen W, Guo G C, Han Z F 2013 *Phys. Rev. A* **87** 062329

[20] Ma X C, Sun S H, Jiang M S, Liang L M 2013 *Phys. Rev. A* **87** 052309

[21] Qin H, Kumar R, Makarov V, Alléaume R 2018 *Phys. Rev. A* **98** 012312

[22] Zhou N R, Zhang T F, Xie X W, Wu J Y 2023 *Signal Process. Image Commun.* **110** 116891

[23] Liao Q, Xiao G, Zhong H, Guo Y 2020 *New J. Phys.* **22** 083086

[24] Weedbrook C 2013 *Phys. Rev. A* **87** 022308

[25] Liao Q, Xiao G, Xu C G, Xu Y, Guo Y 2020 *Phys. Rev. A* **102** 032604

[26] Fossier S, Diamanti E, Debuisschert T, Tualle-Brouri R, Grangier P 2009 *J. Phys. B: At., Mol. Opt. Phys.* **42** 114014

[27] Zhang H, Fang J, He G Q 2012 *Phys. Rev. A* **86** 022338

[28] Wu X D, Wang Y J, Liao Q, Zhong H, Guo Y 2019 *Entropy* **21** 333

[29] Pirandola S, Braunstein S L, Lloyd S 2008 *Phys. Rev. Lett.* **101** 200504

[30] García-Patrón R, Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503

[31] Navascués M, Grosshans F, Acín A 2006 *Phys. Rev. Lett.* **97** 190502

[32] Huang D, Huang P, Lin D K, Zeng G H 2016 *Sci. Rep.* **6** 19201

[33] Huang D, Lin D K, Wang C, Liu W Q, Fang S H, Peng J Y, Huang P, Zeng G H 2015 *Opt. Express* **23** 017511

[34] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E 2013 *Nat. Photonics* **7** 378

[35] Huang L Y, Zhang Y C, Huang Y D, Jiang T W, Yu S 2019 *Phys. B: At. Mol. Opt. Phys.* **52** 225502

[36] Zhang Y C, Li Z Y, Weedbrook C, Yu S, Gu W Y, Sun M Z, Peng X, Guo H 2014 *J. Phys. B: At., Mol. Opt. Phys.* **47** 035501

[37] Guo Y, Li R J, Liao Q, Zhou J, Huang D 2018 *Phys. Lett. A* **382** 372

[38] Blandino R, Leverrier A, Barbieri M, Etesse J, Grangier P, Tualle-Brouri R 2012 *Phys. Rev. A* **86** 012327

[39] Bencheikh K, Lopez O, Abram I, Levenson J A 1995 *Appl. Phys. Lett.* **66** 399

Gaussian-modulated continuous-variable quantum key distribution based on untrusted entanglement source*

Liao Qin [1)] Liu Hai-Jie [1)] Wang Zheng [1)] Zhu Ling-Jin [2)†]

1) (*College of Computer Science and Electronic Engineering, Hunan University, Changsha* 410082, *China*)

2) (*Hunan Institute of Metrology and Test, Changsha* 410014, *China*)

(Received 30 September 2022; revised manuscript received 21 November 2022)

Abstract

In a practical quantum communication system, the security of signal source of continuous-variable quantum key distribution may be jeopardized due to device flaws and hidden attacks. In this paper, an improved scheme for Gaussian-modulated continuous-variable quantum key distribution based on an untrusted entangled source is proposed. In particular, the entanglement source is placed in an untrusted quantum channel to simulate that it is controlled by an eavesdropper, thereby verifying the security of Gaussian-modulated continuous-variable quantum key distribution in a complex environment. This work in detail analyzes the influence of untrusted entanglement source on practical Gaussian-modulated continuous-variable quantum key distribution system, and the numerical simulation shows that the performance of Gaussian-modulated continuous-variable quantum key distribution will dramatically decrease once the entanglement source has moved out of the sender, and it will slightly rise as the untrusted entanglement source slowly moves away from the sender. This paper further introduces two kinds of optical amplifiers, which are phase-sensitive amplifier and phase-insensitive amplifier, to compensate for the imperfection of the coherent detector. These amplifiers are beneficial to enhancing the quantum efficiency of the receiver's detector. Specifically, the security key rate of Gaussian-modulated continuous-variable quantum key distribution with homodyne detection can be well improved by phase-sensitive amplifier, and the security key rate of Gaussian-modulated continuous-variable quantum key distribution with heterodyne detection can be well improved by phase-insensitive amplifier. To summary, this paper proposes a scheme for Gaussian-modulated continuous-variable quantum key distribution with untrusted entanglement source, experimental results show that the proposed scheme can generate secure quantum keys even if the Gaussian entanglement source is untrusted, and the two optical amplifiers can effectively improve the quantum efficiency of the detector at the receiver. This work aims to promote the practical process of the Gaussian-modulated continuous-variable quantum key distribution system and provide theoretical guidance for the practical implementation and application of the Gaussian-modulated continuous-variable quantum key distribution system.

Keywords: continuous-variable quantum key distribution, untrusted entanglement source, optical amplifier, quantum communication

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.72.20221902

* Project supported by the National Natural Science Foundation of China (Grant No. 62101180), the Natural Science Foundation of Hunan Province, China (Grant No. 2022JJ30163), and the State Key Laboratory of High Performance Computing, National University of Defense Technology (Grant No. 202101-25).

† Corresponding author. E-mail: zhulingjin1020@foxmail.com

物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于不可信纠缠源的高斯调制连续变量量子密钥分发

廖骎 柳海杰 王铮 朱凌瑾

Gaussian-modulated continuous-variable quantum key distribution based on untrusted entanglement source

Liao Qin Liu Hai-Jie Wang Zheng Zhu Ling-Jin

引用信息 Citation: Acta Physica Sinica, 72, 040301 (2023) DOI: 10.7498/aps.72.20221902
在线阅读 View online: https://doi.org/10.7498/aps.72.20221902
当期内容 View table of contents: http://wulixb.iphy.ac.cn
